Alert

Prepared by the
Internet Crime Complaint Center (IC3)

January 4, 2006

NEW SOBER WORM EXPECTED TO HIT JANUARY 5, 2006!!!

Reports are circulating regarding the potential release of another Sober Worm, which could have a detrimental affect on Internet traffic as e-mail servers are flooded with politically motivated spam e-mail from potentially tens of millions of e-mail addresses.

iDefense, the cyber security intelligence provider and a VeriSign company, reports the next planned attack of 2005's most prolific e-mail worm family, Sober, is scheduled to start on January 5, 2006, based on commands hard coded within the worm. The attack coincides with the 87th anniversary of the founding of the Nazi party.[1]

iDefense, a Verisign company, provides information regarding security intelligence to the U.S. Government and Global 2000 companies including leaders in financial services, energy, transportation, and telecommunications. The company provides customized, actionable, timely, and relevant intelligence detailing potential threats, vulnerabilities, and security issues directly to C-level executives, general counsels, auditors, senior security managers and staff, and system administrators.[2]

iDefense discovered the next phase of the multi-phased Sober attack by reverse engineering and breaking encrypted code in the most recent Sober variant. This variant first began spreading through the Internet on or about November 16, 2005. The computers infected by the November 16 variant began sending another version on November 22, 2005, to additional computers posing as e-mail from the FBI, The United Kingdom's National High-Tech Crime Unit (NHTCU), German Bundeskriminalamt

[1] VeriSign – "iDefense Exposes Sober Worm Variant Timed With Nazi Party's 87th Anniversary" December 7, 2005 <http://www.verisign.com/press)releases/pr/page)036351.html >.
[2] VeriSign – December 7, 2005

(BKA), and the CIA[3] – see IC3 Alert dated November 22, 2005.

A warning is issued contingent upon the release of this worm, e-mail from various government entities may resurface.

IF YOU RECEIVE A SUSPICIOUS E-MAIL WITH A FILE ATTACHED, DO NOT DOWNLOAD THE ATTACHMENT ASSOCIATED WITH THE E-MAIL. IF YOU RECEIVE THIS E-MAIL OR AN E-MAIL SIMILAR TO THIS, DELETE THE MESSAGE AND DO NOT OPEN THE ATTACHMENT.

[3] VeriSign – December 7, 2005